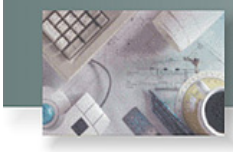

Compliance Component

DEFINITION	
Name	Cryptography for Wireless
Description	Cryptography for Wireless is a way of securing wireless telecommunications. Wireless is defined as a network or terminal that uses electromagnetic waves, (such as radio frequency, infrared, laser, visible light and acoustic energy) for transmission.
Rationale	There is a need for secure electromagnetic access to networks where physical cables are not available and/or feasible.
Benefits	• Assures the confidentiality of broadcast information • Assures the integrity of broadcast information • Improves secured accessibility

ASSOCIATED ARCHITECTURE LEVELS	
List the Domain Name	Security
List the Discipline Name	Technology Controls
List the Technology Area Name	Cryptography
List Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	*NOTE: Bluetooth technology only radiates up to 10 meters, and is therefore not considered a wireless broadcast device under this compliance component.* • Encryption such as Secure Socket Layer (SSL), Secure Shell (SSH) or IPSec shall be used when broadcasting sensitive or critical information requiring confidentiality, reliability and/or authentication over a public access link, such as wireless. • Wireless connections must comply with NIST Special Publication 800-48 • 802.11i Robust Security Network (RSN) encryption must be activated on the access unit. • The WLAN (Wireless Local Area Network) should use at least a 128 bit key. • An external WLAN must use a Virtual Private Network (VPN)

	when connecting to agency networks. • The WLAN must use the Triple Data Encryption Standard (3DES). • The WLAN must use a two-factor authentication scheme. • The WLAN must use Machine Address Code (MAC) authentication or static IP addresses. • The WLAN Service Set IDentifier (SSID) shall not identify the network. Instead, use a long meaningless string of characters or numbers. • The WLAN shall, where appropriate, be set to activate the Broadcast Key Rotation functionality. This will periodically change the communication frequency and impede cracking of the key.		
Document Source Reference #			
Standard Organization			
Name	IEEE	*Website*	http://www.IEEE.org
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	www.csrc.nist.gov/publications/fips/index.html
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	WLANs, X.509, Bluetooth, PDA, 802.11, Palm, Pocket PC, Printers, Blackberry		
COMPONENT CLASSIFICATION			
Provide the Classification	☒ *Emerging* ☐ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			
Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			

CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	01/06/05	*Date Accepted / Rejected*	7/12/05
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	04/07/05
Reason for Update	To incorporate new technology		